



IT Security Handbook

Physical and Environmental Protection

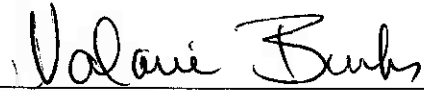
ITS-HBK- 2810.12-01
Effective Date: 20110506
Expiration Date: 20130506
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.12-01)
Physical and Environmental Protection

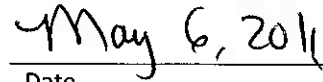
Distribution:

NODIS

Approved



Valarie Burks
Deputy Chief Information Officer for
Information Technology Security



Date

Change History

Version	Date	Change Description
1.0	5/2/11	Initial Draft

Table of Contents

Change History.....	3
1 Introduction and Background	5
2 Physical Access Authorizations (PE-2).....	6
3 Physical Access Control (PE-3)	6
4 Access Control for Transmission Medium (PE-4).....	6
5 Access Control for Output Devices (PE-5).....	6
6 Monitoring Physical Access (PE-6)	6
7 Visitor Control (PE-7)	6
8 Access Records (PE-8)	6
9 Power Equipment and Power Cabling (PE-9).....	7
10 Emergency Shutoff (PE-10)	7
11 Emergency Power (PE-11).....	7
12 Emergency Lighting (PE-12)	7
13 Fire Protection (PE-13).....	7
14 Temperature and Humidity Controls (PE-14)	7
15 Water Damage Protection (PE-15).....	8
16 Delivery and Removal (PE-16).....	8
17 Alternate Work Site (PE-17).....	8
18 Location of Information System Components (PE-18)	8
19 Organizationally Defined Values.....	9

1 Introduction and Background

- 1.1 NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.
- 1.3 *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.4 *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's Physical and Environmental Protection (PE) information security controls.
- 1.5 The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.6 The Physical and Environmental Protection control family relates to the activities and requirements surrounding the development, implementation, and maintenance of physical access authorizations and controls (e.g., key and security badge distribution, visitor management, and related record keeping), and the protection, proofing, and regulation of facilities. NASA protects its facilities and the essential utilities and infrastructure which support those facilities (e.g., door locks, backup power and lighting, emergency plumbing shutoff switches, and fire suppression systems), and also provides appropriate environmental controls for those facilities (e.g., temperature regulation, humidity monitoring). Members of the NASA community are responsible for being aware of, and diligently exercising all facility safety and security procedures.
- 1.7 **Applicable Documents**
- *NPD 2810.1, NASA Information Security Policy*
 - *NPR 1600.1, NASA Security Program Procedural Requirements*
 - *NPR 1620.3, Physical Security Requirements for NASA Facilities and Property*
 - *NPR 2810.1, Security of Information Technology*
 - *NPR 8715.3, NASA General Safety Program Requirements*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *ITS-HBK-0035, Digital Media Sanitization*
 - *ITS-HBK-2810.10-01, Maintenance*
 - *ITS-HBK-2810.11-01, Media Protection*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
 - *American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHREA), Thermal Guidelines for Data Processing Environments*

2 Physical Access Authorizations (PE-2)

2.1 Roles and Responsibilities

2.1.1 *The Information System Owner (ISO) shall:*

- 2.1.1.1 Establish minimum requirements for any individual to obtain credentials for physical access to information systems in a manner consistent with organizationally defined values.
- 2.1.1.2 Establish and maintain a list of individuals authorized to access information systems.
- 2.1.1.3 Ensure that personnel no longer requiring access to the facility are removed from access lists.

3 Physical Access Control (PE-3)

3.1 Roles and Responsibilities

3.1.1 *The ISO shall:*

- 3.1.1.1 Ensure all physical entry and exit points to the facility where information systems reside are controlled (excluding areas in the facility officially designated as publicly accessible).
- 3.1.1.2 Ensure individual access authorization is verified before access is granted to the facility.
- 3.1.1.3 Ensure physical access devices and/or guards are used to control access to the facility.
- 3.1.1.4 Ensure access to areas officially designated as not publicly accessible are controlled.
- 3.1.1.5 Ensure keys and/or combinations to combination locks are stored in a locked container with limited access.
- 3.1.1.6 Ensure for key locks, positive key control is established, key accountability is validated, and that locks are changed when keys are lost in a manner consistent with organizationally defined values.
- 3.1.1.7 Ensure for combination lock access systems, the combinations are managed in a manner consistent with organizationally defined values.
- 3.1.1.8 Ensure compliance with facility processes and procedures when information systems/components are located in a common facility/data center.

4 Access Control for Transmission Medium (PE-4)

- 4.1 NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

5 Access Control for Output Devices (PE-5)

- 5.1 NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

6 Monitoring Physical Access (PE-6)

6.1 Roles and Responsibilities

6.1.1 *The ISO shall:*

- 6.1.1.1 Review information system physical access logs for suspicious physical activities in a manner consistent with organizationally defined values.
- 6.1.1.2 Coordinate results of the reviews and investigation of suspicious activity with the Center Chief Information Security Official (CISO), Organization Computer Security Official (OCSO), Center Chief of Security (CCS), Office of Protective Services (OPS), and the Security Operations Center (SOC).

7 Visitor Control (PE-7)

- 7.1 NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

8 Access Records (PE-8)

8.1 Roles and Responsibilities

- 8.1.1 *The ISO shall:*
 - 8.1.1.1 Ensure visitor access records to non-public areas of facilities where information systems reside are maintained in coordination with the Center CISO, OCSO, CCS, and OPS.
 - 8.1.1.1.1 Visitor access records should contain the name and organization of the visitor, signature of the visitor, forms of identification provided, date of access, time of entry, time of departure, purpose of visit, and the name/organization of person visited.
 - 8.1.1.2 Ensure access records are reviewed, in coordination with the Center CISO, OCSO, CCS, and OPS, in a manner consistent with organizationally defined values.

9 Power Equipment and Power Cabling (PE-9)

- 9.1 NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

10 Emergency Shutoff (PE-10)

10.1 Roles and Responsibilities

- 10.1.1 *The ISO shall:*
 - 10.1.1.1 Ensure facilities, such as data centers, have emergency shutoff capabilities that:
 - 10.1.1.1.1 Are consistent with organizationally defined values, and *NPR 8715.3*.
 - 10.1.1.1.2 Allow the power shutoff to concentrations of information systems or components without requiring individuals to approach the equipment;
 - 10.1.1.1.3 Have emergency switches or devices in the facility at or near the exit door of the facility and/or room of the facility; and
 - 10.1.1.1.4 Are located and protected to prevent shutoff from accidental or unauthorized activation.

11 Emergency Power (PE-11)

- 11.1 NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

12 Emergency Lighting (PE-12)

12.1 Roles and Responsibilities

- 12.1.1 *The ISO shall:*
 - 12.1.1.1 Ensure all facilities in which information systems reside have operational emergency lighting that activates in the event of power outage/disruption that covers emergency exits and evacuation routes within the facility, in accordance with *NPR 8715.3*.

13 Fire Protection (PE-13)

13.1 Roles and Responsibilities

- 13.1.1 *The ISO shall:*
 - 13.1.1.1 Ensure all facilities in which information systems reside have operational fire suppression and detection devices in accordance with *NPR 8715.3*.

14 Temperature and Humidity Controls (PE-14)

14.1 Roles and Responsibilities

- 14.1.1 *The ISO shall:*
 - 14.1.1.1 Ensure temperature and humidity controls are provided and monitored for facilities where information systems reside and maintained, in a manner consistent with organizationally defined values.

15 Water Damage Protection (PE-15)

15.1 NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

16 Delivery and Removal (PE-16)

16.1 Roles and Responsibilities

16.1.1 *The ISO shall:*

16.1.1.1 Ensure the delivery and removal of information system components are authorized, controlled, and a record is maintained, in accordance with organizationally defined values, *ITS-HBK-2810.10-01*, *ITS-HBK-2810.11-01*, and *ITS-HBK-0035*.

17 Alternate Work Site (PE-17)

17.1 NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

18 Location of Information System Components (PE-18)

18.1 NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

19 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
PE	01	Physical and Environmental Protection Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
PE	02	Physical Access Authorizations	Main	[1]	Frequency	Review and approval of access list and authorization credentials.	2/Year	2/Year	2/Year
PE	03	Physical Access Control	Main	[1]	Frequency	Inventory of physical access devices.	2/Year (Key Accountability)	2/Year (Key Accountability)	2/Year (Key Accountability)
PE	03	Physical Access Control	Main	[2]	Frequency	Change of combinations and keys.	1. Change Keys - 1/3-Years 2. Change Combinations - 2/Year	1. Change Keys - 1/3-Years 2. Change Combinations - 2/Year	1. Change Keys - 1/3-Years 2. Change Combinations - 2/Year
PE	06	Monitoring Physical Access	Main	[1]	Frequency	Review of physical access logs.	4/Year	4/Year	1/Month
PE	08	Access Records	Main	[1]	Frequency	Review of visitor access records.	1/Month	1/Month	1/Month
PE	10	Emergency Shutoff	Main	[1]	Reference	Locations where emergency shutoff switches or devices should be placed.		At or near the exit door to the room or facility.	At or near the exit door to the room or facility.

ITS Handbook (ITS-HBK-2810.12-01)
Physical and Environmental Protection

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
PE	14	Temperature and Humidity Controls	Main	[1]	Reference	Acceptable levels for temperature and humidity levels.	Temperature and humidity levels should be consistent with manufacturer recommendations, and/or ASHRAE's Thermal Guidelines for Data Processing Environments.	Temperature and humidity levels should be consistent with manufacturer recommendations, and/or ASHRAE's Thermal Guidelines for Data Processing Environments.	Temperature and humidity levels should be consistent with manufacturer recommendations, and/or ASHRAE's Thermal Guidelines for Data Processing Environments.
PE	14	Temperature and Humidity Controls	Main	[2]	Frequency	Monitoring of temperature and humidity controls.	Continuous	Continuous	Continuous
PE	16	Delivery and Removal	Main	[1]	Reference	Types of components for which controls are in place around the entering and exiting of facilities, and for which records are maintained.	All information system related items including hardware and software components and system software media.	All information system related items including hardware and software components and system software media.	All information system related items including hardware and software components and system software media.

ITS Handbook (ITS-HBK-2810.12-01)
Physical and Environmental Protection

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
PE	17	Alternate Work Site	Main	[1]	Reference	Management, operational, and technical controls employed at alternate work sites.		1. Management Controls: Approved ATO 2. Operational Controls: Alternate work site personnel compliance with the media protection requirements of the NPR 2810.1 policy 3. Technical Controls: Alternate work site personnel compliance with the access control requirements of the NPR 2810.1 policy.	1. Management Controls: Approved ATO 2. Operational Controls: Alternate work site personnel compliance with the media protection requirements of the NPR 2810.1 policy 3. Technical Controls: Alternate work site personnel compliance with the access control requirements of the NPR 2810.1 policy.